IFW.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION

| | | |
|---|---|---|
| Serial No. | : | 10/722,423 |
| Group Art Unit | : | 2616 |
| Examiner | : | YUEN, Kan |
| Title | : | NETWORK BANDWIDTH ANOMALY DETECTOR APPARATUS, METHOD, SIGNALS AND MEDIUM |
| Filing Date | : | November 28, 2003 |
| Inventor/Applicant | : | MACISAAC, Gary Lorne |

March 13, 2009

U.S. Commissioner of Patents and Trademarks
U.S. Patent and Trademark Office
Box 1450
Alexandria, VA 22313-1450
U.S.A.

Sir:

In accordance with 35 U.S.C. 301, Applicant submits the following information to the Examiner in charge of the above-referenced application for patent.

Copies of non-patent references cited as prior art by the Japanese Examiner in a related Japanese Patent Application were submitted with a Supplemental Information Disclosure Statement dated September 30, 2008 and included a reference by Takei, et al (2001). After careful review, the Applicant considers the Takei, et al (2001) reference (English translation: Takei, et al) a significant prior art publication that discloses key elements of the Applicant's present invention. Copies of the two web-based citations and abstracts are enclosed.

Takei, et al discloses a system and method for detecting Denial of Service (DoS) attacks by monitoring and correlating inbound and outbound traffic patterns from given observation points. It is readily apparent there are a number of components in Takei, et al that disclose claims 1, 2, 3, 5, 11, 12, 13, 14, 21, 22, 26, 28, 30, 31, 32, 34, 36, 37, 38, 40 and associated dependent claims in a manner that would be obvious to one of ordinary skill in the art.

Referring to Takei, et al, each of the elements of claims 1, 37, 38 and 40 are disclosed by Takei, et al. Specifically, comparing Figure 8 on page 65 with Figure 9 on page 66, each showing a time distribution of data volume, makes it immediately apparent that the traffic patterns in a first direction (Fig. 8) and a second direction (Fig. 9) are correlated. A method of calculation of a correlation between two time distributions of data volume (time-series) is disclosed on pages 63 and 64 as equations (1) and (2) along with the text description.

Referring to Takei, et al, claims 2 and 3 are disclosed on page 64, in section 2.5 which describes observing traffic patterns in both uplink and downlink directions. Figure 5 illustrates the generation of an anomaly signal based on the outcome of comparing a threshold for a correlation of two patterns of packet counts over time.

In another example, Takei, et al disclose claims 12 and 13 on page 62, column 1, paragraph 5 (last paragraph) where the use of SNMP MIB II statistics is described and notably that their method does not require the extraction and analysis of packet contents thereby providing scalability to higher speed networks.

Although the Applicant's claims include the use of Discrete Wavelet Transform as a statistical measure to be correlated, the key requirement is the comparison of two time distributions of data volumes. On page 62, column 1, paragraph 5 a reference is made to using the "time-series characteristics of the numbers of packets that transit the monitoring points". Transformations simply change the type of time series structure and scales of the packet counts being compared.

In summary, there are many aspects of the newly uncovered prior art of Takei, et al, which reveal features of the present application, such that in view of Takei, et al the Applicant must acknowledge the claims would be obvious to one of average skill in the art.

Respectfully submitted,

Gary Lorne MacIsaac
3708 West 36th Avenue
Vancouver, British Columbia
Canada  V6N 2S4

Encl.

## Detecting and Tracing Illigal Access by using Traffic Pattern Matching Technique.

**Accession number;**01A0745548

**Title;**Detecting and Tracing Illigal Access by using Traffic Pattern Matching Technique.

**Author;**TAKEI YOSUKE(Tohoku Univ., Graduate School of Information Sci., JPN) OTA KOHEI(Cyber Solutions Co., Ltd., JPN) KATO NEI(Tohoku Univ., Graduate School of Information Sci., JPN) NEMOTO YOSHIAKI(Tohoku Univ., Graduate School of Information Sci., JPN)

**Journal Title;**IEICE Transactions on Communications (Japanese Edition)

**Journal Code:**S0622C

**ISSN:**1344-4697

**VOL.J84-B;NO.8;PAGE.1464-1473(2001)**

**Figure&Table&Reference;**FIG.18, TBL.1, REF.18

**Pub. Country;**Japan

**Language;**Japanese

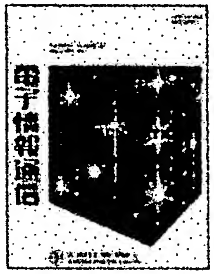
**Abstract;**Recently, illigal access in internet has become a problem. Above all, the illigal access aimed at network itaself gives large effect on whole of the network, rapid establishment of its countermeasure is required. In order to detect this kind of the illigal access, it can be thought that network traffic observation is effective. However, in an illigal access represented by DoS (Denial of Service) it becomes a problem that acquisition and analysis of packet information become difficult by feasibility of manipulation in transmission address of a packet by an attacker and by speed-up of network. Therefore, it is an urgent business to establish an observation method with reliability and low load at future high speed network environment and a method capable of tracing the attacker. This paper proposed an algorithm to detect an illigal access by extracting and comparing change of traffic and showed that by using this algorithm the illigal access could be detected and traced.

BACK

My Profile Log In Athens Log In

English translation of Takei et al (2001)

Home / Engineering / Electrical and Electronics Engineering



Electronics and Communications in Japan (Part I: Communications)

Volume 87 Issue 1, Pages 61 - 71

Published Online: 9 Sep 2003

- Get Sample Copy
- Recommend to Your Librarian
- Save journal to My Profile
- Set E-Mail Alert
- Email this page
- Print this page
- RSS web feed (What is RSS?)

Save Article to My Profile Download Citation <Previous Abstract | Next Abstract>

**Abstract** | References | Full Text: PDF (Size: 1241K) | Related Articles | Citation Tracking

## Detecting and tracing illegal access by using traffic pattern matching technique

Yohsuke Takei [1], Kohei Ohta [2], Nei Kato [1], Yoshiaki Nemoto [1]

[1] GSIS, Tohoku University, Sendai, 980-8579 Japan

[2] Cyber Solutions, Inc., Sendai, 989-3204 Japan

### Keywords

illegal access detection • DoS attack • IP spoofing • traffic pattern • high-speed network

### Abstract

Illegal access on the Internet has become a problem in recent years. Since illegal access aimed at the network significantly affects the entire network, there has been an urgent need to establish countermeasures. Observing network traffic is considered an effective means for detecting this type of illegal access. However, problems presented by the kinds of illegal access represented by a DoS (Denial of Service) attack are that the attacker can alter the packet source address. Acquiring and analyzing packet information is also difficult due to the increased network speed. Therefore, there is an urgent need to establish a reliable and low-impact observation technique and a technique that enables attackers to be traced in future high-speed network environments. In this paper, the authors propose an algorithm for detecting illegal access by extracting and comparing changes in traffic patterns and show that illegal access can be detected and traced by applying this algorithm. © 2003 Wiley Periodicals, Inc. Electron Comm Jpn Pt 1, 87(1): 61-71, 2004; Published online in Wiley InterScience (www.interscience.wiley.com). DOI